Abstraction Refinement with Path Constraints for Three-Valued Bounded Model Checking
– Proofs –

Nils Timm and Stefan Gruner

Department of Computer Science, University of Pretoria, Pretoria, South Africa
{ntimm,sgruner}@cs.up.ac.za

In this technical report we present the proofs of Theorem 1, Theorem 2 and Theorem 3 of the article *Abstraction Refinement with Path Constraints for Three-Valued Bounded Model Checking*, submitted to the *Sixth International Workshop on Formal Techniques for Safety-Critical Systems*. In the proofs we make use of Proposition 1, proven in [1], which states that definite (*true* and *false*) temporal logic properties are preserved under three-valued abstraction refinement.

Proposition 1. *Let $Sys = \|_{i=1}^{n} P_i$ over Var be a concurrent system. Let A_a and A_r be sets of atomic predicates over Var with $A_a \subset A_r$. Let M_a be the three-valued Kripke structure modelling the state space of Sys abstracted over A_a, and let M_r be the three-valued Kripke structure modelling the state space of Sys abstracted over A_r. Moreover, let ψ be a BTL formula and $k \in \mathbb{N}$ be a bound. Then the following holds:*

1. ${}_{A_a}[M_a \models_\exists \psi]_k = \mathit{true} \;\Rightarrow\; {}_{A_r}[M_r \models_\exists \psi]_k = \mathit{true}$
2. ${}_{A_a}[M_a \models_\exists \psi]_k = \mathit{false} \;\Rightarrow\; {}_{A_r}[M_r \models_\exists \psi]_k = \mathit{false}$

The first theorem that we will prove here is as follows:

Theorem 1. *Let $input = (Sys, Init, \psi, k)$ be an tuple consisting of a system, an initial state predicate, a safety formula and a bound. Then the following holds:*

1. $AR(input) = \mathit{true}$ *iff* $WRC(input) = \mathit{true}$
2. $AR(input) = \mathit{false}$ *iff* $WRC(input) = \mathit{false}$

Proof of Theorem 1.
The correctness of Theorem 1 follows from the following:

1. If an unconfirmed witness ω can be proven to be spurious in the inner loop of *WRC*, then it is sound to add the corresponding spurious witness constraint $\overline{\sigma}(\omega)$ to the model checking problem in the outer loop. Here soundness means that there exist a level of abstraction characterised by some predicate set A such that for all further refinements characterised by $A' \supseteq A$ model checking with and without the constraint will yield the same result, i.e. the result is not affected by $\overline{\sigma}(\omega)$ (Lemma 1).
2. If using an unconfirmed witness constraint $\sigma(\omega)$ in the inner loop of *WRC* yields a *true* result, then we would also obtain a *true* result without using this constraint (Lemma 2).

Lemma 1. *Let ${}_{A^\omega}[M \models_\exists \psi]_k$ be a three-valued bounded model checking problem. Moreover, let ω be a spurious witness and $\sigma(\omega)$ be the corresponding constraint. Then the following holds:*

$${}^{\{\sigma(\omega)\}}_{A^\omega}[M \models_\exists \psi]_k = \mathit{false} \;\Rightarrow\; \exists\, A \text{ with } \forall\, A' \supseteq A : \left({}^{\varnothing}_{A'}[M \models_\exists \psi]_k \;\equiv\; {}^{\{\overline{\sigma}(\omega)\}}_{A'}[M \models_\exists \psi]_k\right)$$

Proof of Lemma 1.

$$\begin{aligned}
& {}^{\{\sigma(\omega)\}}_{A^\omega}[M \models_\exists \psi]_k = \mathit{false} && \text{(Premise)}\\
\equiv\; & {}^{\varnothing}_{A^\omega}[M \models_\exists \psi \wedge \sigma(\omega)]_k = \mathit{false} && \text{(Def. 4 and 5)}\\
\equiv\; & {}^{\varnothing}_{A^\omega}[M \models_\forall \neg\psi \vee \overline{\sigma}(\omega)]_k = \mathit{true} && \text{(Def. 6, Correspondence between ex. and univ. Model Checking)}
\end{aligned}$$

We now use the result of this equivalence transformation as a new premise:

$$\begin{aligned}
& {}^{\varnothing}_{A^\omega}[M \models_\forall \neg\psi \vee \overline{\sigma}(\omega)]_k = \mathit{true} && \text{(Premise)}\\
\Rightarrow\;& \forall A' \supseteq A^\omega : {}^{\varnothing}_{A'}[M \models_\forall \neg\psi \vee \overline{\sigma}(\omega)]_k = \mathit{true} && \text{(Proposition 1)}\\
\Rightarrow\;& \forall A' \supseteq A^\omega : {}^{\varnothing}_{A'}[M \models_\exists \psi]_k \;\equiv\; {}^{\varnothing}_{A'}[M \models_\exists \psi \wedge (\neg\psi \vee \overline{\sigma}(\omega))]_k && \text{(Conj. of } \psi \text{ with univ. valid property)}\\
\Rightarrow\;& \forall A' \supseteq A^\omega : {}^{\varnothing}_{A'}[M \models_\exists \psi]_k \;\equiv\; {}^{\varnothing}_{A'}[M \models_\exists \psi \wedge \overline{\sigma}(\omega)]_k && \text{(Equivalence transformation)}\\
\Rightarrow\;& \forall A' \supseteq A^\omega : \big({}^{\varnothing}_{A'}[M \models_\exists \psi]_k \;\equiv\; {}^{\{\overline{\sigma}(\omega)\}}_{A'}[M \models_\exists \psi]_k\big) && \text{(Def. 4, 5, 6)}\\
\Rightarrow\;& \exists\, A \text{ with } \forall A' \supseteq A : \big({}^{\varnothing}_{A'}[M \models_\exists \psi]_k \;\equiv\; {}^{\{\overline{\sigma}(\omega)\}}_{A'}[M \models_\exists \psi]_k\big) && (A := A^\omega)
\end{aligned}$$

The result of this implication completes the proof of Lemma 1. □

Lemma 2. *Let ${}_{A^\omega}[M \models_\exists \psi]_k$ be a three-valued bounded model checking problem. Moreover, let ω be a spurious witness and $\sigma(\omega)$ be the corresponding constraint. Then the following holds:*

$${}^{\{\sigma(\omega)\}}_{A^\omega}[M \models_\exists \psi]_k = \mathit{true} \;\Rightarrow\; {}^{\varnothing}_{A^\omega}[M \models_\exists \psi]_k = \mathit{true}$$

Proof of Lemma 2.

$$\begin{aligned}
& {}^{\{\sigma(\omega)\}}_{A^\omega}[M \models_\exists \psi]_k = \mathit{true} && \text{(Premise)}\\
\equiv\;& {}^{\varnothing}_{A^\omega}[M \models_\exists \psi \wedge \sigma(\omega)]_k = \mathit{true} && \text{(Def. 4, 5, 6)}\\
\equiv\;& {}^{\varnothing}_{A^\omega}[M \models_\exists \psi]_k = \mathit{true} \;\wedge\; {}^{\varnothing}_{A^\omega}[M \models_\exists \sigma(\omega)]_k = \mathit{true} && \text{(Def. 4)}\\
\equiv\;& {}^{\varnothing}_{A^\omega}[M \models_\exists \psi]_k = \mathit{true} && \text{(Equivalence transformation)}
\end{aligned}$$

The result of this implication completes the proof of Lemma 2. □

The correctness of Theorem 1 follows from Lemma 1 and Lemma 2. □

Next, we prove Theorem 2:

Theorem 2. *Let $\mathit{input} = (\mathit{Sys}, \mathit{Init}, \psi, k)$ be an tuple consisting of a system, an initial state predicate, a safety formula and a bound. Then the following holds:*

1. $\mathit{AR}(\mathit{input}) = \mathit{true}$ *iff* $\mathit{SAT\text{-}WRC\text{-}UC}(\mathit{input}) = \mathit{true}$
2. $\mathit{AR}(\mathit{input}) = \mathit{false}$ *iff* $\mathit{SAT\text{-}WRC\text{-}UC}(\mathit{input}) = \mathit{false}$

Proof of Theorem 2.
We already have that *WRC* yields the same results as *AR* (Theorem 1) and that also *SAT-WRC* yields the same results as *AR* (Corollary 1). Consequently the following implication, which reformulates Lemma 1 in the SAT setting, holds:

$$\begin{gathered}
\mathbf{sat_3}\big({}_{A^\omega}[\![M,\psi,k]\!] \cup [\![\sigma(\omega)]\!]\big) = \mathit{false}\\
\Rightarrow\\
\exists\, A \text{ with } \forall A' \supseteq A : \Big(\mathbf{sat_3}\big({}_{A'}[\![M,\psi,k]\!]\big) \;=\; \mathbf{sat_3}\big({}_{A'}[\![M,\psi,k]\!] \cup \overline{[\![\sigma(\omega)]\!]}\big)\Big)
\end{gathered}$$

According to this implication, it is sound to use SAT-encoded *spurious witness constraints* $\overline{[\![\sigma(\omega)]\!]}$ as constraints of the overall encoded model checking problem. We still need to show that the same holds for encoded *spurious fragment constraints* $\overline{[\![\sigma(\omega)]\!]}_{uc}$, which follows from Lemma 3:

Lemma 3. *Let ${}_{A^\omega}[\![M,\psi,k]\!]$ the encoding of a three-valued bounded model checking problem. Moreover, let ω be a spurious witness and $\sigma(\omega)$ be the corresponding constraint. Then the following holds:*

$$\mathbf{sat_3}\big({}_{A^\omega}[\![M,\psi,k]\!] \cup [\![\sigma(\omega)]\!]\big) = \mathit{false}$$
$$\Rightarrow$$
$$\exists\, A \textit{ with } \forall\, A' \supseteq A : \Big(\mathbf{sat_3}\big({}_{A'}[\![M,\psi,k]\!]\big) \;=\; \mathbf{sat_3}\big({}_{A'}[\![M,\psi,k]\!] \cup \overline{[\![\sigma(\omega)]\!]}_{uc}\big)\Big)$$

Proof of Lemma 3.

$$\begin{aligned}
& \mathbf{sat_3}\big({}_{A^\omega}[\![M,\psi,k]\!] \cup [\![\sigma(\omega)]\!]\big) = \mathit{false} && \text{(Premise)}\\
\Rightarrow\;& \mathbf{sat_3}\big({}_{A^\omega}[\![M,\psi,k]\!] \cup [\![\sigma(\omega)]\!]_{uc}\big) = \mathit{false} && \text{(Def. 10)}\\
\Rightarrow\;& \begin{pmatrix} \mathbf{sat_3}\big({}_{A^\omega}[\![M,\psi,k]\!]\big) = t \;\Rightarrow\; \mathbf{sat_3}\big({}_{A^\omega}[\![M,\psi,k]\!] \cup \overline{[\![\sigma(\omega)]\!]}_{uc}\big) = t \\ \mathit{and} \\ \mathbf{sat_3}\big({}_{A^\omega}[\![M,\psi,k]\!]\big) = f \;\Rightarrow\; \mathbf{sat_3}\big({}_{A^\omega}[\![M,\psi,k]\!] \cup \overline{[\![\sigma(\omega)]\!]}_{uc}\big) = f \end{pmatrix} && \text{(three-valued equiv. transf.)}\\
\Rightarrow\;& \exists\, A \text{ with } \forall\, A' \supseteq A : \Big(\mathbf{sat_3}\big({}_{A'}[\![M,\psi,k]\!]\big) = \mathbf{sat_3}\big({}_{A'}[\![M,\psi,k]\!] \cup \overline{[\![\sigma(\omega)]\!]}_{uc}\big)\Big) && \text{(Prop. 1)}
\end{aligned}$$

The result of this implication completes the proof of Lemma 3. □

The correctness of Theorem 2 follows from Lemma 3 (together with Theorem 1 and Corollary 1). □

Next, we prove Theorem 3:

Theorem 3. *Let $[\![\sigma(\omega)]\!]_{uc}$ be an initial state independent encoding of the spurious fragment of ω that was generated in bound iteration k.*

1. *Then it is admissible to reuse the constraint $\overline{[\![\sigma(\omega)]\!]}_{uc}$ in iterations $k' \geq k$.*
2. *Moreover, position shifts of $\overline{[\![\sigma(\omega)]\!]}_{uc}$ within the bound are also admissible constraints in $k' \geq k$.*

Proof of Theorem 3.
The correctness of Part 1 of Theorem 3 follows from Lemma 4 (Combined with Lemma 3). Moreover, we make use of the fact that an encoding, e.g. $[\![\sigma(\omega)]\!]_{uc}$, can be decoded back into a BTL formula $\mathit{btl}([\![\sigma(\omega)]\!]_{uc})$ (Def. 7 in [3]).

Lemma 4. *Let ${}_{A^\omega}[\![M,\psi,k]\!]$ the encoding of a three-valued bounded model checking problem. Moreover, let ω be a spurious witness and $\sigma(\omega)$ be the corresponding constraint. Then the following holds:*

$$\mathbf{sat_3}\big({}_{A^\omega}[\![M,\psi,k]\!] \cup [\![\sigma(\omega)]\!]_{uc}\big) = \mathit{false} \textit{ and } [\![\sigma(\omega)]\!]_{uc} \textit{ initial state independent}$$
$$\Rightarrow$$
$$\mathbf{sat_3}\big({}_{A^\omega}[\![M,\psi,k+1]\!] \cup [\![\sigma(\omega)]\!]_{uc}\big) = \mathit{false}$$

Proof of Lemma 4.

$$\begin{aligned}
& \mathbf{sat_3}\big({}_{A^\omega}[\![M,\psi,k]\!] \cup [\![\sigma(\omega)]\!]_{uc}\big) = \mathit{false} \text{ and } [\![\sigma(\omega)]\!]_{uc} \text{ initial state independent} && \text{(Premise)}\\
\Rightarrow\;& \mathbf{sat_3}\big({}_{A^\omega}[\![R,k]\!] \cup [\![\sigma(\omega)]\!]_{uc}\big) = \mathit{false} && \text{(Def. 12)}\\
\Rightarrow\;& \text{There exist no path segment of length } k \text{ in } M, && \text{(Encoding Def. [2])}\\
& \text{starting in an arbitrary state, that satisfies } \mathit{btl}([\![\sigma(\omega)]\!]_{uc}).\\
\Rightarrow\;& \text{there exist no path prefix of length } k+1 \text{ in } M, && \text{(Deduction)}\\
& \text{starting in an initial state, that satisfies } \mathit{btl}([\![\sigma(\omega)]\!]_{uc}).\\
\Rightarrow\;& \mathbf{sat_3}\big({}_{A^\omega}[\![M,\psi,k+1]\!] \cup [\![\sigma(\omega)]\!]_{uc}\big) = \mathit{false} && \text{(Encoding Def. [2])}
\end{aligned}$$

The result of this implication completes the proof of Lemma 4. □

The correctness of Part 2 of Theorem 3 follows from Lemma 5 (Combined with Lemma 3):

Lemma 5. *Let ${}_{A^\omega}[\![M,\psi,k]\!]$ the encoding of a three-valued bounded model checking problem and let ω be a spurious witness with the corresponding path constraint $\sigma(\omega)$. Moreover, let $[\![\sigma(\omega)]\!]_{uc}$ be the unsatisfiable core of the encoded constraint with the corresponding BTL formula $btl([\![\sigma(\omega)]\!]_{uc}) = \sigma_i \wedge \ldots \wedge \sigma_j$ with $0 \leq i \leq j \leq k$ where σ_i refers to the i-indexed part of the formula.*

Then the following holds:

$$\mathbf{sat_3}\big({}_{A^\omega}[\![M,\psi,k]\!] \cup [\![\sigma(\omega)]\!]_{uc}\big) = \mathit{false} \ \text{ and } [\![\sigma(\omega)]\!]_{uc} \text{ initial state independent}$$
$$\Rightarrow$$
$$\forall\, l \text{ with } -i \leq l \leq k-j : \Big(\mathbf{sat_3}\big({}_{A^\omega}[\![M,\psi,k]\!] \cup [\![\sigma_{i+l} \wedge \ldots \wedge \sigma_{j+l}]\!]\big) = \mathit{false}\Big)$$

Proof of Lemma 5.

$$\begin{array}{lll}
 & \mathbf{sat_3}\big({}_{A^\omega}[\![M,\psi,k]\!] \cup [\![\sigma(\omega)]\!]_{uc}\big) = \mathit{false} \text{ and } [\![\sigma(\omega)]\!]_{uc} \text{ initial state independent} & \text{(Premise)} \\
\Rightarrow & \mathbf{sat_3}\big({}_{A^\omega}[\![R,k]\!] \cup [\![\sigma(\omega)]\!]_{uc}\big) = \mathit{false} & \text{(Def. 12)} \\
\Rightarrow & \text{There exist no path segment } \pi_i \ldots \pi_j \text{ of a } k\text{-bounded path in } M, & \text{(Encoding Def. [2])} \\
 & \text{starting in an arbitrary state, that satisfies } \sigma_i \wedge \ldots \wedge \sigma_j. & \\
\Rightarrow & \text{There exist no path segment } \pi_{i+l} \ldots \pi_{j+l} \text{ of a } k\text{-bounded path in } M, & \text{(Deduction)} \\
 & \text{starting in an arbitrary state, that satisfies } \sigma_{i+l} \wedge \ldots \wedge \sigma_{j+l}, & \\
 & \text{where } -i \leq l \leq k-j. & \\
\Rightarrow & \forall\, l \text{ with } -i \leq l \leq k-j : \Big(\mathbf{sat_3}\big({}_{A^\omega}[\![M,\psi,k]\!] \cup [\![\sigma_{i+l} \wedge \ldots \wedge \sigma_{j+l}]\!]\big) = \mathit{false}\Big) & \text{(Encoding Def. [2])}
\end{array}$$

The result of this implication completes the proof of Lemma 5. □

The correctness of Theorem 3 follows from Lemma 4 and Lemma 5. □

References

1. Timm, N., Gruner, S.: Three-valued bounded model checking with cause-guided abstraction refinement (2018), manuscript submitted for publication
2. Timm, N., Gruner, S., Harvey, M.: A bounded model checker for three-valued abstractions of concurrent software systems. In: Ribeiro, L., Lecomte, T. (eds.) Formal Methods: Foundations and Applications. pp. 199–216. Springer (2016)
3. Timm, N., Gruner, S., Harvey, M.: Constraint reusing and k-induction for three-valued bounded model checking. In: Massoni, T., Mousavi, M. (eds.) Formal Methods: Foundations and Applications. Springer (2018)